Peter Mayer, Alexandra Kunz, Melanie Volkamer

Analyse der Sicherheit und Erinnerbarkeit der DsiN-Passwortkarte

Das Wählen und Merken angemessen sicherer Passwörter stellt für viele Benutzer ein Problem dar. Die Passwortkarte der Initiative „Deutschland sicher im Netz“ wurde vorgeschlagen, um Benutzern bei der Bewältigung dieses Problems zu helfen. Sie besteht aus einem Raster mit zufällig angeordneten Buchstaben, Zahlen und Symbolen. Aus diesem Raster wählen die Benutzer einen Startpunkt und von diesem ausgehend einen Verlauf über jeweils benachbarte Felder. Das Passwort besteht aus den Buchstaben, Zahlen und Symbolen entlang des Verlaufs. Der Beitrag analysiert die Sicherheit und Erinnerbarkeit von Passwörtern, die mithilfe dieser Passwortkarte erstellt wurden. Die Untersuchung zeigt, dass Benutzer meist vorhersagbare Verläufe und Startpunkte wählen. Zugleich erwies sich die Erinnerbarkeit der gewählten Startpunkte und Verläufe bereits nach kurzer Zeit als niedrig.

1 Einleitung

Textpasswörter sind die häufigste Form der Authentifizierung. Jedoch stellen sie Benutzer vor die Herausforderung, Passwörter zu wählen, die einerseits schwer zu erraten aber andererseits einfach zu merken sind [8]. Dies ist besonders für KMU relevant, die besonders häufig zum Ziel von Angriffen werden [9]. Ansätze, um Benutzer bei dieser Problematik zu unterstützen, beinhalten sowohl elektronische Hilfsmittel wie Passwortmanager [6] als auch analoge Hilfsmittel wie das Aufzeichnen von Passwörtern in Notizbüchern [4]. Während in der wissenschaftlichen Literatur die Sicherheit und Benutzbarkeit von Passwortmanagern ausgiebig untersucht wurden, sind analoge Hilfsmittel ein weithin unerforschtes Gebiet [10].

In dieser Arbeit wird die Sicherheit und Erinnerbarkeit von Passwörtern bei einer konkreten analogen Maßnahme betrach-tet: der Passwortkarte der Initiative „Deutschland sicher im Netz“ (DsiN, im Folgenden kurz DsiN-Passwortkarte). Sie ist eine Kar-te aus Papier im Kreditkartenformat und besteht aus einem Ras-ter mit zufällig angeordneten Buchstaben, Zahlen und Symbolen. Um ein Passwort zu erstellen, wählt der Benutzer zunächst einen beliebigen Startpunkt innerhalb des Rasters und bildet von dort aus einen Verlauf über benachbarte Felder (siehe Abb. 1).

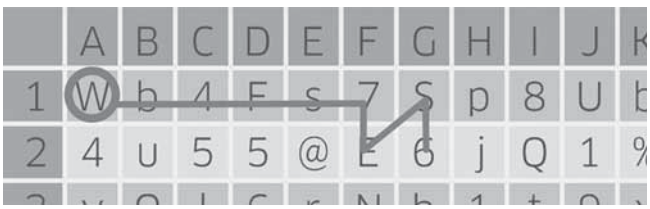
Wir haben die Sicherheit und Erinnerbarkeit dieses Ansatzes in einer Benutzerstudie mit 30 Teilnehmern untersucht. Unsere Ergebnisse zeigen, dass die vorrangig gewählten Verläufe aus geraden, horizontalen Linien bestehen und dass die gewählten Startpunkte der Teilnehmer nicht zufällig im Raster verteilt liegen. Darüber hinaus erweist sich die Erinnerbarkeit der Verläufe selbst nach kurzer Zeit als niedrig.

2 Die Passwortkarte

Die Passwortkarte soll Benutzer bei dem Wählen und Merken angemessen sicherer Textpasswörter unterstützen [7]. Sie besteht aus einem Raster mit zufällig angeordneten Buchstaben, Zahlen und Symbolen (siehe Abb. 2). Das Raster wird von einem Koordinatensystem eingeschlossen, dessen x-Achse von links nach rechts mit den Buchstaben A bis Z und dessen y-Achse von oben nach unten mit den Zahlen 1 bis 12 versehen ist. Da die Anordnung der Buchstaben, Zahlen und Symbole im Raster unveränderlich ist und somit für jeden Benutzer dieselbe, stellt die Verfügbarkeit der Karte bei Verlust kein Problem dar, ebenso wie die Geheimhaltung der Karte. Jedoch hängt somit die Sicherheit der Passwörter lediglich vom gewählten Startpunkt und Verlauf ab.

Um ein Passwort mit der Karte zu erstellen, wählt der Benutzer zunächst einen beliebigen Startpunkt innerhalb des Rasters aus und bildet von dort aus einen Verlauf über benachbarte Felder. Laut den auf der Karte aufgedruckten Anweisungen sollte sich der Verlauf über mindestens acht Felder erstrecken. Die Zeichen der Felder im Verlauf bilden das neue Passwort (siehe Abb. 1 für ein Beispiel). Die Anleitung zur Passwortbildung befi ndet sich am unteren Rand der Karte unter dem Raster sowie auf der Rückseite der Karte.

Abbildung 1 | Beispielhafter Verlauf auf der Passwortkarte und das zugehörige Passwort "Wb4Fs7ES6"



3 Methode

Um die Sicherheit und die Erinnerbarkeit von Passwörtern, die mit Hilfe der Passwortkarte gebildet wurden, zu untersuchen, haben wir eine Benutzerstudie durchgeführt. Die Studie entspricht den Standards der Ethikkommission der Technischen Universität Darmstadt. Die Teilnehmer wurden in der Fußgängerzone und Parkanlagen sowie über Mundpropaganda für die Studie angeworben. Insgesamt nahmen 30 Personen an der Studie teil. Jeder Teilnehmer erhielt 5 € als Aufwandsentschädigung. Die Studie bestand aus fünf Phasen und dauerte für jeden Teilnehmer ungefähr 20 Minuten.

- **Phase 1:** Die Teilnehmer erhielten eine kurze Einführung zur Passwortkarte. Im An-schluss erhielten die Teilnehmer eine Pass-wortkarte und hatten Zeit, um sich mit die-ser und deren Benutzung vertraut zu ma-chen (dies schloss auch das Lesen der Infor-mationen auf der Rückseite mit ein).
- **Phase 2:** Nachdem sich die Teilnehmer mit der Passwortkarte vertraut gemacht hatten, erhielten sie einen ersten Fragebogen und sollten angeben, ob sie die Passwortkarte bereits kannten und, falls dies der Fall war, ob sie diese auch benutzen.
- **Phase 3:** Anschließend wurden die Teilnehmer beauftragt, mit Hilfe der Passwortkarte drei Passwörter für die drei Verwendungszwecke Haupt-E-Mail-Adresse, Online Banking und Online-Forum zu erstellen. Die drei Passwörter sollten dabei nacheinander auf drei leeren Passwortkarten eingetragen werden. Die Teilnehmer wurden angewiesen, die Passwörter entsprechend der Anweisungen auf der Passwortkarte zu erstellen, d. h. einen beliebigen Startpunkt auszuwählen und von dort aus einen Verlauf über mindestens acht Felder zu wählen. Die Teilnehmer markierten den Startpunkt mit einem Kreis und den Verlauf mit einer Linie durch die entsprechenden Kästchen des Rasters (siehe Abb. 1 für ein Beispiel). Anschließend wurden die Karten vom Versuchsleiter eingesammelt.
- **Phase 4:** Nach Erstellung der Passwörter wurden die Teilnehmer aufgefordert, einen zweiten Fragebogen als Ablenkung auszufüllen, welcher unter anderem Fragen zu demographischen Daten beinhaltete (z. B. Alter, Geschlecht) und weitere Fragen bezüglich der Benutzung der Passwortkarte (z. B. ob sie die Passwortkarte zukünftig benutzen würden). Der Fragebo-gen nahm etwa fünf bis 10 Minuten Zeit in Anspruch.
- **Phase 5:** Zum Abschluss wurden die Teilnehmer gefragt, ob sie sich noch an die drei zuvor gewählten Startpunkte und die zugehörigen Verläufe erinnerten. Um diese Aussage zu überprüfen, mussten die Teilnehmer ihre Passwörter auf drei leeren Passwortkarten einzeichnen, analog zu Phase 3. Anschließend wurden die Teilnehmer noch zu den Gründen bei der Wahl ihrer Startpunkte und Verläufe befragt. Schließlich wurden die Teilnehmer über den Zweck der Studie aufgeklärt und erhielten ihre Aufwandsentschädigung.

4 Ergebnisse

Die Stichprobe war relativ gleich verteilt in Bezug auf das Geschlecht (13 männliche und 17 weibliche Teilnehmer). Das Alter der Teilnehmer reichte von 19 bis 70 Jahren mit einem Mittelwert von 34,2 Jahren.

Abbildung 2 | Heatmap aller gewählten Startpunkte der Teilnehmer in unserer Studie

4.1 Sicherheit

Die Sicherheit der mit der Passwortkarte erstellten Passwörter hängt davon ab, ob (a) die Startpunkte zufällig im Raster verteilt liegen und ob (b) die Verläufe nicht vorhersagbar sind.

Verteilung der Startpunkte: Um die Verteilung der Startpunkte zu untersuchen, verwenden wir die räumliche *J(r)* Statistik wie in [2] für Sicherheitsanalysen vorgeschlagen. Dabei bezeichnet *r* den Radius um jeden Startpunkt, auf dessen Grundlage die Verteilung im Raster berechnet wird:

- *J(r)*-Werte nahe 1 geben eine zufällige Verteilung der Startpunkte an (was für Passwort-Sicherheit wünschenswert ist).
- *J(r)*-Werte unter 1 deuten auf Clustering der Startpunkte hin.
- *J(r)*-Werte über 1 deuten auf räumliche Regelmäßigkeit hin.

Mit *J(2)* = 0.785 scheint unsere Analyse auf ein Clustering hinzudeuten. Die Heatmap in Abb. 2 zeigt die Verteilung der Startpunkte. Eine Ungleichverteilung der Startpunkte mit einer Tendenz zur linken Seite wird deutlich. Die Antworten der Teilnehmer bezüglich der Wahl ihrer Startpunkte geben zusätzliche An-haltspunkte für die Interpretation der Ergebnisse.

Die Koordinaten der Startpunkte wurden oft mit einem Bezug zum entsprechenden Be-nutzerkonto gewählt: *„Für den Startpunkt des Bankpassworts wähle ich ‚B' und ‚9', weil ‚B'* für Bank steht u*nd meine Kontonummer mit einer ‚9' beginnt"* (T3), „[Ich habe] *versucht Anfangs-punkte so zu wählen, dass man sie sich sicher merken kann (B [für] Banking, E [für] E-Mail, 3 [da] Geburtstag...)."* (T8). Andere Teilneh-mer benutzten persönliche Informationen oder persönliche Erfahrungen für die Wahl ihrer Startpunkte: *„Um die Koordinaten auszuwählen, habe ich den ersten Buchstaben meines Namens und eine Zahl aus meinem Geburtsdatum gewählt"* (T18), *„Ich habe für die Koordinate meines E-Mail-Passworts meine Glückszahl ausgesucht"* (T20). Andere hingegen gaben an, die Startpunkte völlig zufällig gewählt zu haben.

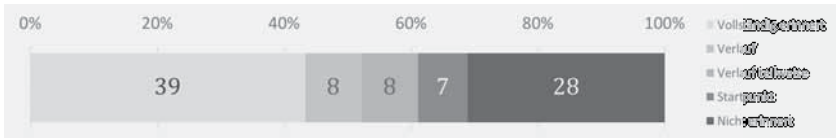
Vorhersagbarkeit der Verläufe: Betrachtet man die Verläufe der Passwörter, zeigt sich, dass die große Mehrheit lediglich aus vertikalen oder horizontalen Bewegungen besteht (83,3%). Verläufe mit diagonalen Bewegungen stellen die Ausnahme dar (16,7%). Zudem ändert die Mehrheit der Verläufe nie ihre Richtung (41,1%), das heißt sie bestehen aus geraden Linien (23,3% horizontale, 10,0% vertikale, 7,8% diagonale Linien). Die meisten der horizontalen und diagonalen Linien verlaufen von links nach rechts. 22,2% der Verläufe ändern ihre Richtung nur einmal (für Details siehe Abbildung 3). Wieder geben die Antworten der Teilnehmer weiteren Aufschluss über die Gründe zur Wahl der Verläufe. Diese drehen sich hierbei vor allem um den Aspekt der Erinnerbarkeit: *„Die Zeichen im Raster sind bereits zufällig angeordnet, deshalb muss der Verlauf es nicht auch noch sein. Deshalb habe ich eine gerade Linie gewählt, weil diese für mich leichter zu merken ist."* (T28), *"Ich habe eine gerade Linie gewählt, weil ich es mir einfacher merken kann."* (T30).

Abbildung 3 | Die Häufigkeit in Abhängigkeit zur Anzahl an Richtungsänderungen der Verläufe

4.2 Erinnerbarkeit

Die Mehrheit der Passwörter konnte in Phase 5 ca. zehn Minuten nach der Erstellung von den Teilnehmern nicht mehr reproduziert werden: Nur 43,3% der Passwörter wurden von den Teilnehmern vollständig erinnert, 31,1% konnten gar nicht erinnert werden (siehe Abb. 4 für Details). Dabei stimmte nur bei 58,9% der Passwörter die Einschätzung der Teilnehmer mit ihrer tatsächlichen Erinnerbarkeit überein (betreff end die Kategorien aus Abb. 4). Die Annahme der Teilnehmer, sich gerade Linien bes-ser merken zu können, wird von den Ergebnissen der Analyse auch nicht gestützt. Eine Überprüfung mit Fishers exaktem Test konnte hier keinen signifi kanten Unterschied zwischen der Er-innerbarkeit von geraden Linien und anderen Verläufen aufzei-gen (FET: p = 0.829).

Abbildung 4 | Die Häufigkeit in Abhängigkeit zum Grad, zu welchem sich die Teilnehmer an ihre Passwörter erinnern



5 Fazit

Unsere Analyse der DsiN-Passwortkarte deutet auf eine geringe Erinnerbarkeit der Startpunkte und Verläufe nach nur fünf bis zehn Minuten hin. Auch hinsichtlich Sicherheitsaspekten kann die Passwortkarte nicht überzeugen. Ähnlich zu Sicherheitsanalysen von anderen Ansätzen [1, 2] identifizieren wir Probleme:

- Die Startpunkte sind nicht zufällig im Raster verteilt und
- die meisten Verläufe in unserer Studie sind gerade Linien oder beinhalten lediglich eine Richtungsänderung.

Daher scheint die Passwortkarte kein geeignetes Hilfsmittel zur Unterstützung von Benutzern bei dem Wählen und Merken von angemessen sicheren Passwörtern zu sein.

Die Fortführung dieser Arbeit beinhaltet die Überprüfung unserer Ergebnisse mit einer größeren Stichprobe in einer On-line-Studie. Des Weiteren könnte basierend auf einer größeren Stichprobe ein spezialisierter Rate-Algorithmus entwickelt und evaluiert werden.

Danksagung

Diese Arbeit wurde im Rahmen des Projekts „KMU AWARE" der Initiative ‚IT-Sicherheit in der Wirtschaft ' des Bundesministeriums für Wirtschaft und Energie fi nanziert. Die Initiative ‚IT-Sicherheit in der Wirtschaft ' des Bundesministeriums für Wirtschaft und Energie will vor allem kleine und mittelstän-dische Unternehmen beim sicheren Einsatz

von IKT-Systemen unterstützen. Gemeinsam mit IT-Sicherheitsexperten aus Wissenschaft, Wirtschaft und Verwaltung soll eine Grundlage dafür geschaffen werden, um die Bewusstseinsbildung in der digitalen Wirtschaft beim Thema IT-Sicherheit im Mittelstand zu stärken. Unternehmen sollen durch konkrete Unterstützungsmaßnahmen dazu befähigt werden, ihre IT-Sicherheit zu verbessern. Weitere Informationen zur Initiative und ihren Ange-boten sind unter www.it-sicherheit-in-der-wirtschaft.de abrufbar.

Literatur

[1] Adam J Aviv, Devon Budzitowski, and Ravi Kuber. *Is Bigger Better? Comparing User-Generated Passwords on 3x3 vs. 4x4 Grid Sizes for Android's Pattern Unlock*. In Annual Computer Security Applications Conference. ACM, 2015, 301–310.

[2] S Chiasson, E Stobert, A Forget, R Biddle, and P C van Oorschot. *Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge- Based Authentication Mechanism*. IEEE Transactions on Dependable and Secure Computing 9, 2 (2012), 222–235.

[3] Sonia Chiasson, Paul C van Oorschot, and Robert Biddle. *A Usability Study and Critique of Two Password Managers*. In USENIX Security Symposium, 2006, 1–16.

[4] Vijay Kothari, Ross Koppel, Jim Blythe, and Sean Smith. *Password Logbooks and What Their Amazon Reviews Reveal About Their Users' Motivations, Beliefs, and Behaviors*. In European Workshop on Usable Security, 2017.

[5] Zhiwei Li, Warren He, Devdatta Akhawe, and Dawn Song. *The Emperor's New Password Manager: Security Analysis of Web-based Password Managers*. In USENIX Security Symposium, 2014. 465–479.

[6] Daniel McCarney, David Barrera, Jeremy Clark, Sonia Chiasson, and Paul C van Oorschot. *Tapas: design, implementation, and usability evaluation of a password manager*. In Annual Computer Security Applications Conference, 2012. 89–98.

[7] Reinhard Muth. *Die Passwortkarte*. https://www.dsin-blog.de/2013/08/20/ die-passwortkarte/. (2013). Accessed: 2017-06-21.

[8] Elizabeth Stobert and Robert Biddle. *The Password Life Cycle: User Be-haviour in Managing Passwords*. In Symposium on Usable Privacy and Security, 2014.

[9] Verizon. *2017 Data Breach Investigations Report*.

[10] Andreas Dähn. Kennwortkarten. In Datenschutz und Datensicherheit (DuD), 10/2015, S. 692–695.